AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Utah

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
See Attachment A

Case No. 2:18mj597-RTB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, information associated with wrightkeith365@gmail.com stored at premises owned, maintained, controlled, or operated by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA, 94043.

located in the Northern Division District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252, 2252A	Receipt, Distribution, Transportation, Reproduction and Possession of Child Pornography.

The application is based on these facts:

See Affidavit Attached Hereto and Incorporated by Reference Herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

James Wright, SA, Homeland Security Investigations
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/16/2018

Judge's signature

City and state: Salt Lake City, Utah

Robert T. Braithwaite, United States Magistrate Judge
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH
Central Division

IN THE MATTER OF THE SEARCH OF:	)	
	)	
	)	**Case No. _____**
See Attachment A	)	
	)	

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, James Wright, a Special Agent (SA) with the Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the HSI since February 2004, and I am currently assigned to the HSI Salt Lake City Office of the Assistant Special Agent in Charge (ASAC) and work with local, state, and other federal law enforcement agencies. While employed by HSI, I have investigated federal criminal violations related to violent crimes against children, including child exploitation and child pornography. I have gained experience through training at the HSI Cyber Crimes Center (C3) in Fairfax, Virginia, and the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by the Attorney General to request a search warrant.

FACTS AND CIRCUMSTANCES

3. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to the Google, Inc. account **wrightkeith365@gmail.com** associated with CECIL KEITH WRIGHT("SUBJECT ACCOUNT"), the contents of this Gmail account and associated records residing with Google Legal Investigations Support, 1600 Amphitheatre Parkway, Mountain View, CA 94043 which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code §§ 18 U.S.C. §§ 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt and distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(3)(B) and (b)(1) (sale and possession with intent to sell a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt and distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography); which items are more specifically described in Attachment B.

4. The statements in this affidavit are based in part on information obtained and provided by Weber County Sheriff's Office (WCSO) and Adult Probation & Parole (AP&P) and

from my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt and distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(3)(B) and (b)(1) (sale and possession with intent to sell a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt and distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography) are located in the SUBJECT ACCOUNT.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a "district court of the United States (including a magistrate judge of such court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of the following:

   a. Title 18, United States Code, Sections 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

   b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

   c. Title 18, United States Code, Sections 2252(a)(3)(B) and (b)(1) prohibit any person from knowingly selling or possessing with the intent sell, or attempting or

conspiring to sell or possessing with the intent to sell, any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or has been shipped or transported in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported using any means or facility of interstate or foreign commerce, including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

e. Title 18, United States Code, Sections 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce

by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

f. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

g. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond

quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

e. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

f. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

k. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

l. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

m. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality;

(c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

n. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

o. "Webcam," as used herein, refers to a front-facing video camera that attaches to a computer or that is built into a laptop or desktop screen. It is widely used for video calling as well as to continuously monitor an activity and send it to a Web server for public or private viewing. Webcams generally have a microphone built into the unit or use the computer's microphone for audio.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent

of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e.,

"Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Gmail and Hotmail, among

others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

ONLINE SEXUAL EXPLOITATION OF CHILDREN VIA SOCIAL MEDIA, EMAIL AND THE INTERNET

9. Based on my training and experience, I know of ways that individuals entice, coerce and exploit children and minors online for the purpose of illicit sexual conduct. Based on my training and experience working child exploitation investigations and online enticement

investigations, individuals will look and seek minors, both male and female and make contact with them for the purpose of engaging in illicit sexual conduct with those minors.

10. Individuals use email, social media and messaging applications (apps) to facilitate their enticement of those minors. Individuals begin with non-sexual messages and build a relationship with the minors eventually turning the conversation sexual and requesting "selfies" of the minor either partially nude, completely nude or performing a sex act.

TECHNICAL INFORMATION REGARDING GMAIL

Gmail E-mail

11. Based on my training and experience, and publicly available information, I have learned that Google, Inc. provides a variety of on-line services, including e-mail access, to the general public. Google, Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain a Gmail email account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, e-mail transaction information, and account application information.

12. In general, an e-mail that is sent to a Google, Inc. subscriber is stored in the subscriber's "mail box" on Google, Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google, Inc.'s servers indefinitely. The user can move and store messages in personal folders such as a "sent folder."

In recent years, Google, Inc., and other ISPs have provided their users with larger storage capabilities associated with the user's e-mail account. Google, Inc., and other ISPs have allowed users to store up to one (1) terabyte of information associated with the account on ISP servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search warrants of e-mail accounts, I have learned that search warrants for e-mail accounts and computer systems have revealed stored e-mails sent and/or received many years prior to the date of the search.

13. When the subscriber sends an e-mail, it is initiated at the user's computer or mobile device, transferred via the Internet to Google, Inc.'s servers, and then transmitted to its end destination. Google, Inc. typically saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google, Inc. server, the e-mail can remain on the system indefinitely.

14. A sent or received e-mail typically includes the content of the message (including attachments), source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google, Inc. but may not include all of these categories of data.

15. A Google, Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google, Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

16. Many subscribers to Google, Inc. do not store copies of the e-mails stored in their Google, Inc. account on their home computers. This is particularly true because they access their Google, Inc. account through the Internet, and thus it is not necessary to copy e-mails to a home computer to use the service. Moreover, an individual may not wish to maintain particular e-mails or files in their residence to ensure others with access to the computer cannot access the e-mails.

17. In my training and experience, generally, e-mail providers like Google, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers (usually a mobile number) and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

18. The mobile number and alternate e-mail information provided to Google, Inc., by the user are particularly useful in instances where a user needs to recover his/her account in the event of a lost password or account compromise. With these, Google, Inc. can send a "reset password" link to the alternate e-mail address, or an SMS message to the mobile number. Upon receiving the "reset password" link to an SMS mobile number affiliated with that account, the user can then reset the password in order to continue to utilize that particular account. Because

both a mobile device number and alternate e-mail address are used to recover access to an account, they both tend to be closely associated with the user of the account. It is important to note that though Gmail attempts to validate the personal identifying information provided by subscribers, the validation requires additional voluntary input from users. As this additional input is voluntary, Gmail is not always successful in validating a user's personal identifying information.

19. When creating an account at Google, Inc., the user is provided the opportunity to create a display name and an associated "Profile." Google, Inc. allows a user to personalize their Profile by "adding an image that represents you." The display name and display image a user provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users.

20. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google, Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

21. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. In my training and experience, e-mail users often use e-mail accounts for everyday transactions because it is fast, low cost, and simple to use. People use e-mail to communicate with friends and family, manage accounts, pay bills, and conduct other online business. E-mail users often keep records of these transactions in their e-mail accounts, to include personal identifying information such as name and address.

23. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored in the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

BACKGROUND OF THE INVESTIGATION

25. On or about September 12, 2018, WRIGHT was taken into custody for violation of his parole agreement with AP&P. Upon being taken into custody, a laptop computer owned and belonging to WRIGHT was seized.

26. On or about September 12, 2018, Detective Cameron Hartman, WCSO requested my assistance to examine the hard drive of the laptop, based on the parole agreement has WRIGHT with AP&P.

27. On or about September 12, 2018, Special Agent (SA) James Wright, HSI Salt Lake City, examined the contents of the hard drive and found seven still images files in the following location: **Windows\Users\Owner\Pictures\iCloud Photos\Downloads**.

28. On or about September 12, 2018, SA Wright and Detective Hartman looked at the seven (7) images with the following descriptions:

- "0550D3C1-CAAE-4C33-86D3-84CA5A5A71AF-2925 00001DDF5E98388.jpeg"

  This is a still image file of what appears to be a prepubescent female with her genitalia exposed to the camera
- "2E817FE9-0204-4113-B0C0-B8DBA3E3F1E5-2925-000001B73DC415C5.jpeg"

  This is a still image file of what appears to be a prepubescent female, nude, with her finger in her vagina.
- "5A693747-893B-FD91-B059-1FDC7CAB373F-2925-000001DC6F17FFBB.jpeg"

  This is a still image of what appears to be a prepubescent female, with her buttocks exposed.
- "6C03C3D9-1796-42A8-8098-222A31F80BFE-2925-000001DBCB27F844.jpeg"

This is a still image file of what appears to be a nude prepubescent female facing the camera with genitalia exposed.

- "6D966752-4C9A-4CC6-ABCE-3D05296BD38C-2925-000001D64C0FEE.jpeg"

  This is a still image file of what appears to be a nude prepubescent female, facing the camera, with unseen adult male, with erect penis having anal intercourse with the female.

- "C8DA04EB-B220-44EC-8FCD-9D3A93CEFAD2-2925-000001D64245E534.jpeg

  This is a still image file of what appears to be two nude prepubescent females, with one having their genitalia exposed, involved in sexual activities.

- "D173F053-484E-4C36-A6A5-1B9B8A20ADDB-2925-000001DBC3521F86.jpeg"

  This is a still image file of what appears to be a partially nude prepubescent female with her genitalia exposed.

29. It is believed that WRIGHT used online accounts and user profiles to access, download, and possess child pornography.

30. On or about September 21, 2018, a preservation letter was submitted to Google Legal Investigations Support to preserve the contents of WRIGHT'S Gmail account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

32. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Google, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic account described in Attachment A. The facts outlined above show that the SUBJECT ACCOUNT listed in Attachment A has been used to produce child pornography, receive visual depictions of a minor engaged in sexually explicit conduct, possession and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct, receipt, possession and distribution of child pornography, and coercion and enticement. There is probable cause to believe that the user of the SUBJECT ACCOUNT used the SUBJECT ACCOUNT to violate the aforementioned statutes in the District of Utah.

33. Because the warrant will be served on Google, Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

34. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court, except that a copy of the warrant, including its attachments, shall be served upon Google, Inc. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

James P. Wright
Special Agent
Homeland Security Investigations

Sworn and Subscribed before me this 16th day of October, 2018.

ROBERT J. BRAITHWAITE
United States Magistrate Judge

Reviewed by:

Cristina P. Ortega
Assistant United States Attorney

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with wrightkeith365@gmail.com, a Gmail email account that is stored at premises controlled by Google, Inc., a company that accepts service of legal process at Google Legal Investigations Support, 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Gmail (the "Provider") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc. , including any emails, records, files, logs, or information that have been deleted but are still available to Google, Inc. , or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 24, 2017, Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in that email account which is helpful to determine the account user's or owner's true identity:

a. The contents of all e-mails associated with the account, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each e-mail;

b. The contents of all Instant Messages (IM) associated with the account, from the time of account creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP

address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between Google, Inc. and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to:

SA JAMES WRIGHT
HSI Salt Lake City
2975 South Decker Lake Drive
West Valley City, Utah 84119
james.p.wright@ice.dhs.gov

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after August 4, 2015, that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. § 2251(a), (c), and (e) (production and attempted production of child pornography); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt and distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(3)(B) and (b)(1) (sale and possession with intent to sell a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of child pornography); and 18 U.S.C. § 2422(b) (coercion and enticement), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;

b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;

c. Any person knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged, or attempting to do so;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the email account owner or user;

e. Evidence indicating the email account user's or owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the account or identifier listed on Attachment A was used;

5. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc. , and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. Such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc. ; and

c. Such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature